DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE 1/21

PHYSICAL SECURITY STANDARDS FOR SENSITIVE COMPARTMENTED INFORMATION FACILITIES

(Effective 1 September 1987)

Pursuant to the provisions of Section 102 of the National Security Act of 1947 and Executive Order 12333, physical security standards for sensitive compartmented information facilities (SCIFs) are hereby established.

1. Purpose

The purpose of this directive is to establish minimum construction and security protection standards required for all US Government facilities or US Government-sponsored contractor facilities where sensitive compartmented information (SCI) may be stored, used, discussed, and/or processed.

2. General

All SCI must be stored within accredited SCIFs. Accreditation is the formal affirmation that the proposed facility meets, or exceeds, the minimum physical security standards imposed by the DCI in the physical security standards manual that supplements this directive. The DCI is the accrediting authority for all SCIFs except where that authority has been delegated or otherwise provided for (see DCID 1/19).

3. Applicability

This directive is applicable to all SCIFs. Senior Officials of the Intelligence Community (SOICs) are charged with implementation and enforcement of the provisions of this directive. SCIFs established in all organizations outside the cognizance of Intelligence Community agencies/departments as defined in Executive Order 12333 are directly under the authority and oversight of the DCI. SCIFs are established exclusively for SCI and are intended to provide the highest level of physical security protection. It is sometimes necessary for non-SCI programs to be afforded an equal level of protection by introduction of such material into SCIFs. Should this occur, the express approval of the accrediting authority is required, and appropriate documentation shall be included in the accreditation records.

4. Policy

SOICs shall establish and maintain within their agencies formal physical security programs to ensure that SCI is properly protected. The minimum physical security requirements for such protection are contained in *Physical Security Standards for Sensitive Compartmented Information Facilities*, the supplement to this directive. Annexes to this manual addressing specific technical and tactical applications of standards shall be published separately and periodically updated as required.

5. Interpretation

Questions concerning the interpretation and implementation of SCIF physical security standards shall be referred to the Community Counterintelligence and Security Countermeasures Office/Intelligence Community Staff (CCISCMO/ICS).

APPROVED FOR RELEASE
DATE: NOV 2000

MANUAL FOR PHYSICAL SECURITY STANDARDS FOR SENSITIVE COMPARTMENTED INFORMATION FACILITIES (SCIFs)

Supplement to DCID 1/21

(Effective 1 September 1987)

APPROVED FOR RELEASE
DATE: NOV 2000

TABLE OF CONTENTS

NOTE: This manual supersedes NFIB/NFIC-9.1/47 dated 23 April 1981 "US Intelligence Community Physical Security Standards for Sensitive Compartmented Information Facilities.

APPROVED FOR RELEASE
DATE: NOV 2000

POLICY STATEMENT

Physical security standards are hereby established governing the construction and protection of facilities for storing and processing sensitive compartmented information (SCI) [1] that requires extraordinary security safeguards as prescribed in pertinent national directives. These regulations also cover electric or electronic equipment located in sensitive compartment information facilities (SCIFs). Compliance with these standards is mandatory for all facilities established after the effective date of DCID 1/21, including any renovation of existing facilities insofar as the renovation will permit reasonable and practical upgrading. It is not intended that existing, previously approved facilities be modified to conform to these standards. Facilities that meet these standards are satisfactory for the storage of all SCI.

It is recognized that there may be instances in which circumstances constitute a threat of such proportion that it can only be offset by the most stringent security arrangements. Conversely, there may arise those instances in which time, location, condition of use of the material, or other unforeseen factors may render full compliance with these standards unreasonable or impossible. Situations such as the foregoing are to be referred to the accreditation authority as far in advance as possible in order that full and timely consideration may be given to a request for deviation from the standards. When these standards are waived, the accreditation authority granting the waiver will inform the SCIF manager which elements of security protection must be strengthened before the SCIF can meet acceptable minimum standards. For industrial contractor-operated SCIFs, waivers are valid only for the duration of the contract. The fact of a waiver condition will be made known by the Cognizant Security Authority to other agencies/departments desiring to share use of the facility.

The physical security standards set forth in this manual are intended as minimum safeguards for protection of SCI. Senior Officials of the Intelligence Community (SOICs) are authorized to impose more stringent standards for SCIFs if conditions and circumstances in certain areas constitute potential threats that justify additional protective measures.

All facilities must be accredited before SCI may be stored in them. The procedures for establishment and accreditation of SCIFs are prescribed in applicable national directives.

[1] SCI as used in this directive is classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled exclusively within formal access control systems established by the Director of Central Intelligence.

APPROVED FOR RELEASE
DATE: NOV 2000

SECTION I

DEFINITIONS

ACCESS CONTROL SYSTEM, UNATTENDED

An electronic, electromechanical, or mechanical system designed to identify and/or admit personnel with properly authorized access to the secure area. Identification may be based on any number of factors such as the sequencing of a combination, special key, badge, fingerprints, signature, voice, etc. These systems are for personnel access control only and are not to be used for the protection of classified materials.

ACCREDITATION

Formal certification by a cognizant security authority (CSA) of a specific place (to be referred to as a SCIF) that meets prescribed physical and technical security standards.

ACOUSTIC SECURITY

Those security measures designed and used to deny aural access to classified information.

ADMINISTRATIVE/SERVICE AREAS

Those identified areas within an accredited SCIF where storage, discussion, and/or processing of SCI is not allowed.

AUTHORIZED PERSONNEL

Any person who is fully cleared and indoctrinated for SCI, has a valid need-to-know, and has been granted access to the SCIF.

CLOSED STORAGE

The storage of SCI material in properly secured GSA-approved security containers within an accredited SCIF when the SCIF is not occupied.

COGNIZANT SECURITY AUTHORITY (CSA)

Government agency responsible for the accreditation and general security of a SCIF.

CONTINUOUS OPERATIONS

This condition exists when a facility is manned 24 hours every day by not fewer than two appropriately indoctrinated personnel who have the continuous capability of detecting unauthorized entry into the SCIF. Positive identification and access control must be maintained at all entrance points not fully secured.

CONTINUOUS PERSONNEL ACCESS CONTROL

An access control system where access to a facility is continuously controlled by a cleared individual, as determined by the CSA.

CONTROLLED AREA

Any area to which entry is subject to restrictions or control for security reasons.

APPROVED FOR RELEASE
DATE: NOV 2000

DOCUMENT

Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, paintings, drawings, photos, engravings, sketches, working notes and papers, reproductions of such things by any means or process, and sound, voice, magnetic, or electronic recordings in any form.

GUARD

A properly trained and equipped individual whose duties include the protection of a SCIF. Guards whose duties require direct access to a SCIF or patrol within a SCIF must meet the clearance criteria in DCID 1/14. The CSA will determine if indoctrination is required.

INTRUSION DETECTION SYSTEM

A security alarm system consisting of various types of components (balanced magnetic switches, capacitance, infrared, ultrasonic, etc.) to detect intrusion in the area of coverage within a facility.

MOTION DETECTION SYSTEM

An alarm sensor that detects movement or human presence within a SCIF.

NONDISCUSSION AREA

A clearly defined area within a SCIF where classified discussions are not authorized. All such areas will be clearly marked.

OPEN STORAGE

The maintenance of SCI material within a SCIF in any configuration other than within GSA-approved security containers.

SCI FACILITY (SCIF)

An accredited area, room, group of rooms, or installation where SCI may be stored, used, discussed, and/or electronically processed.

SECURE WORKING AREA

An accredited facility used for handling, discussing, and/or processing of SCI but where SCI will not be stored.

SENIOR OFFICIAL OF THE INTELLIGENCE COMMUNITY (SOIC)

Those senior principals and observers on the National Foreign Intelligence Board who head intelligence organizations or intelligence-producing agencies within the Intelligence Community.

SENSITIVE COMPARTMENTED INFORMATION (SCI)

SCI is classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled exclusively within formal control systems established by the Director of Central Intelligence.

APPROVED FOR RELEASE
DATE: NOV 2000

SOUND GROUPS

Voice transmission attenuation groups established to satisfy the acoustical security requirements of SCIFs. Ratings measured in sound transmission class may be found in Chapter 13 of *Architectural Graphic Standards*.

SOUND TRANSMISSION CLASS (STC)

The rating used in architectural considerations of sound transmission loss such as those involving walls, ceilings, and/or floors.

SURREPTITIOUS ENTRY

The unauthorized entry into a SCIF or security container in a manner in which evidence of such entry is not readily discernible.

TACTICAL OR COMBAT OPERATIONS

Operations that are conducted under combat or simulated combat conditions (to include ground, airborne, and shipboard) and that must provide for a mobile or nonpermanent SCIF environment.

TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM) SURVEYS AND INSPECTIONS

A thorough physical, electronic, and visual examination to detect technical surveillance devices, technical security hazards, and attempts at clandestine penetration of the facility for hostile technical collection of classified and sensitive information.

TEMPORARY SECURE WORKING AREA (TSWA)

A temporarily accredited facility that is used no more than 40 hours monthly for handling, discussing, and/or processing of SCI, but where SCI will not be stored.

VAULT

A room(s) used for storing, handling, discussing, and/or processing SCI and constructed to afford maximum protection against unauthorized entry.

VISUAL SECURITY

Those security measures designed and used to deny unauthorized visual access to classified materials and activity.

VOLUMETRIC SENSORS

An alarm sensor that detects movement or human presence within a SCIF.

APPROVED FOR RELEASE
DATE: NOV 2000

SECTION II

GENERAL

A. SCI FACILITIES

A SCIF is an accredited area, room, group of rooms, or installations where SCI may be stored, used, discussed, and/or electronically processed. SCIFs will be afforded personnel access control to preclude entry by unauthorized personnel. Non-SCI-indoctrinated personnel entering a SCIF must be continuously escorted by an indoctrinated employee who is familiar with the security procedures of that SCIF. The physical security protection for a SCIF is intended to prevent as well as detect visual, acoustical, technical, and physical access by unauthorized persons. Entrance doors to SCIFs must be limited to one. If extraordinary circumstances require more than one door, appropriate justification must be approved by the CSA. Physical security criteria is governed by whether the SCIF is in the United States or not, and whether it is located at, above, or below ground level according to the following conditions: closed storage, open storage, continuous operations, secure working areas, nondiscussion areas, and administrative/service areas.

B. TWO-PERSON RULE

As a matter of policy, SCIFs should be staffed with sufficient people to deter unauthorized copying or illegal removal of SCI. Communication centers, document control areas, and like facilities that handle or store quantities of SCI must be manned while in operation by at least two appropriately indoctrinated persons in such proximity to one another as to provide mutual support in maintaining the integrity of the facility and the material stored therein. The granting of exceptions to this policy will be made a matter of record by the CSA and should involve consideration of the proven reliability and maturity of the persons involved; the volume, variety, and sensitivity of the holdings in the facility; and whether or not the persons involved are subject to periodic polygraph examinations as a condition of access. Exceptions for communication centers, document control areas, and the like, should be granted in only extraordinary circumstances. Classified work by a lone individual in any SCIF is to be avoided. Contractors will provide two-person occupancy in all SCIFs not specifically excepted by the CSA.

C. SOUND ATTENUATION

All SCIFs must meet the sound attenuation requirements as set forth in Chapter 13 of *Architectural Graphic Standards.*

D. CO-UTILIZATION

Agencies desiring to co-utilize a SCIF should accept the accreditation of the facility as determined by the CSA. Exceptions to this policy are valid only when significant deviations from DCID 1/21 standards exist or when the co-utilizing agency requires security enhancements at the facility in connection with an especially sensitive program. All proposed security enhancements must be fully coordinated with the CSA prior to implementation.

E. INSPECTIONS

A SCIF inspection every two years by the CSA or designated representative is required to certify continued compliance with DCID 1/21; however, an annual SCIF inspection is strongly recommended.

APPROVED FOR RELEASE
DATE: NOV 2000

SECTION III

CONSTRUCTION POLICY FOR SCI FACILITIES

A. GENERAL

Physical security criteria is governed by whether the SCIF is in the United States or not, and whether it is located at, above, or below ground level according to the following conditions: closed storage, open storage, continuous operations, and secure working areas.

B. SCI FACILITIES LOCATED IN THE UNITED STATES AT GROUND LEVEL

1. Closed Storage

a. The SCIF must meet the specifications as listed in Section V.A.4 or meet open storage requirements. SCIFs within fenced, guarded military compounds, or equivalent may use specifications described in Section V.A.2.

b. The SCIF must be alarmed in accordance with Section IV.

c. SCI material must be stored in GSA-approved security containers.

2. Open Storage

a. Open storage of SCI material will be avoided. When open storage is necessary, the SCIF must meet either:

(1) The construction specifications for vaults set forth in Section V.A.1 and must be alarmed in accordance with Section IV; or

(2) The construction specifications for SCIFs set forth in Section V.A.4 and must be alarmed in accordance with Section IV and be located in a building that has all of the following:

(a) continuous personnel access control,

(b) a 24-hour guard force capable of responding to an alarm within five minutes, and

(c) a reserve guard force available to assist the responding guard in an emergency.

b. SCIFs within fenced, guarded military compounds or equivalent may use specifications indicated in Section V.A.2 and must be alarmed in accordance with Section IV and be located in a building that has all the requirements cited by paragraph B.2.(b) above.

3. Continuous Operations

a. The SCIF must meet the construction specifications as identified in Section V.A.2 and have an alert system as stated in Section IV if visual security observation of the SCIF door(s) and other potential points of entry (i.e., windows and ducts) is not feasible.

b. An adequate security/guard force must be available to respond to the SCIF within five minutes in an emergency.

APPROVED FOR RELEASE
DATE: NOV 2000

c. Provision should be made for storage of SCI in lockable containers. If the configuration of the material precludes this, there must be an adequate, tested plan to protect, evacuate, or destroy the material in event of emergency or natural disaster.

4. Secure Working Areas

a. The SCIF must meet the specifications set forth in Section V.A.2.

b. The SCIF must be alarmed in accordance with Section IV.

C. SCI FACILITIES LOCATED IN THE UNITED STATES ABOVE OR COMPLETELY BELOW GROUND LEVEL

1. Closed Storage

a. The SCIF must meet the specifications specified in Section V.A.2 or meet open storage requirements.

b. The SCIF must be alarmed in accordance with Section IV.

c. SCI must be stored in GSA-approved security containers.

2. Open Storage

Open storage of SCI will be avoided. When open storage is necessary, the SCIF must meet either:

a. The construction specifications for vaults set forth in Section V.A.1 and must be alarmed in accordance with Section IV; or

b. The construction specifications for SCIFs as set forth in Section V.A.2 and must be alarmed in accordance with Section IV and be located in a building that has all of the following:

(1) continuous personnel access control,

(2) a 24-hour guard force capable of responding to an alarm within five minutes, and

(3) a reserve guard force available to assist the responding guard in an emergency.

3. Continuous Operation

a. The SCIF must meet the construction specifications identified in Section V.A.2 and have an alert system as stated in Section IV if visual security observation of the SCIF door(s) and other potential points of entry (i.e., windows and ducts) is not feasible.

b. An adequate security force must be available to respond to the SCIF within five minutes in an emergency.

c. Provision should be made for storage of SCI in lockable containers. If the configuration of the material precludes this, there must be an adequate, tested plan to protect, evacuate, or destroy the material in the event of emergency or natural disaster.

4. Secure Working Areas

a. The SCIF must meet the specifications stipulated in Section V.A.2.

b. The SCIF must be alarmed in accordance with Section IV.

APPROVED FOR RELEASE
DATE: NOV 2000

D. SCI FACILITIES LOCATED OUTSIDE THE UNITED STATES

The criteria for SCIFs outside the US are the same as those for SCIFs within the US except as follows:

1. Closed Storage

a. The SCIF must meet the construction specifications for SCIFs as set forth in Section V.A.3. SCIFs within fenced, guarded military compounds, or equivalent of "friendly" host countries, having armed, immediate response forces may use specifications indicated in Section V.A.4, with prior approval of the SOIC.

b. All SCI-controlled material will be stored in GSA-approved security containers having a rating for both forced and surreptitious entry equal to or exceeding that afforded by Class 5 containers.

c. The SCIF must be alarmed in accordance with Section IV.

2. Open Storage

a. No waiver will be granted for the construction requirement (Section V.A.1) of a vault approved for open storage.

b. Open storage of SCI will be permitted only for material that is of a size or configuration that precludes its being stored in the largest GSA-approved security container available. All other SCI must be stored in a GSA-approved security container having a rating for both forced and surreptitious entry equal to or exceeding that afforded by Class 5 containers.

c. The SCIF must be alarmed in accordance with Section IV.

3. Continuous Operations

a. The SCIF must meet the construction specifications indicated in Section V.A.3 and have an alert system as stated in Section IV if visual security of the SCIF door(s) and other potential points of entry (i.e., windows and ducts) is not feasible.

b. Capability must exist for storage of all SCI in GSA-approved security containers, or the SCIF must have an adequate, tested plan to protect, evacuate, or destroy the material in the event of emergency or natural disaster.

c. SCIFs located on controlled military reservations or equivalent in "friendly" host countries, having armed, immediate response forces, may use secure area construction specifications as listed in Section V.A.2, with prior approval of the SOIC.

APPROVED FOR RELEASE
DATE: NOV 2000

SECTION IV

SECURITY ALARM REQUIREMENTS

A. All SCIFs, except those in continuous operation, must be alarmed. Continuous operation SCIFs will have an alert system if visual security of the SCIF door(s) and other potential points of entry (i.e., windows and ducts) is not feasible.

B. SCIFs located **within the United States** may use commercial monitoring facilities for alarm systems if approved by the CSA. Response to an alarm should not exceed 10 minutes. When a commercial central station is used, a UL-rated, Class A service is required. (This response statement does not apply to open storage or continuous operations requirements that specify five minutes or less.)

C. SCIFs located **outside the United States** must have alarm systems monitored by SCI-cleared personnel or US citizens.

D. Alarm installation and maintenance should be accomplished by US citizens. Use of foreign nationals for this purpose must have prior CSA approval, and all work must be done under close supervision of SCI cleared personnel or US citizens.

E. In SCIFs where the alarm transmission signal leaves the facility and traverses **an uncontrolled area**, Class A line supervision will be used. Class A line supervision is a wire-transmitted, nonrepeatable, or encrypted signal, meeting the requirements of federal standard 1027.

F. In SCIFs where the alarm transmission signal does not leave a **controlled area** containing the SCIF, Class A or Class B line supervision may be used. Class B line supervision is a repeatable or unencrypted signal, wire transmitted.

G. All SCIF alarm systems will include the following:

1. Alarm components, when not specified by CSA, will be UL-approved.
2. All areas of the SCIF between the floor and ceiling will be protected by volumetric sensors.
3. If a SCIF has a false ceiling or floor that provides a means for surreptitious entry, one of the following methods must be used to protect that area:
   a. A separate alarm zone in secure mode at all times covering the area between the false and true ceiling or false and true floor.
   b. Construction of a physical barrier that replaces the false ceiling or floor equal to the SCIF wall construction as set forth in Section V.
4. Perimeter doors will be protected by balanced or biased magnetic switches.
5. All windows will be protected by an alarm system, either independently or by the volumetric sensors in the room, as determined by the CSA.
6. Emergency exits and secondary doors will be on separate zones from the motion detecting and main entrance sensors within the same SCIF.
7. Every SCIF will be on a separate system.

APPROVED FOR RELEASE
DATE: NOV 2000

8. If a SCIF consists of more than six rooms, or more than 5,000 square feet, it will be protected by two or more alarm zones as determined by the CSA.
9. All alarm control units will be located **within** the SCIF.
10. All alarm sensors will be tested monthly, i.e., doors opened and volumetric sensors walk-tested. Test procedures will be prepared and recorded by the SCIF security officer or as directed by the CSA.
11. All components will be installed in a manner to prevent access or removal from a location external to the protected zone.
12. All alarm systems will be capable of operating from commercial AC power. In the event of commercial power failure, provisions will be made for automatic switchover to emergency power, and back to commercial power without causing an alarm. A signal will be presented to the monitor location indicating when the system has lost all power. When batteries are used for emergency power, they will be maintained at full charge by automatic charging circuits. Emergency power must be capable of operating the system for a minimum of six hours.
13. Volumetric sensors employed in the alarm system must be placed so that the most likely paths of an intruder are detected.
14. All sensors and control units will be equipped with tamper detection.

H. Details concerning classes of electronic line supervision, equipment type, specific component application and response/service requirements will be addressed in the technical annex attached or furnished by the CSA.

I. Alert System—An alert system will consist of balanced magnetic switches or other appropriate sensors on all entrances and passages or other areas where undetected entry could occur. These sensors will be connected to a signaling device through a closed loop to a latching relay. Neither the signaling device, relay, nor the wire connecting the switches will leave the SCIF.

APPROVED FOR RELEASE
DATE: NOV 2000

SECTION V

CONSTRUCTION

A. SPECIFICATIONS

1. Vault Construction Criteria

a. ***Reinforced Concrete Construction.*** Walls, floor, and ceiling will be a minimum thickness of eight inches of reinforced concrete. The concrete mixture will have a comprehensive strength rating of at least 3,000 psi. Reinforcing will be accomplished with steel reinforcing rods, a minimum of 5/8 inches in diameter, positioned centralized in the concrete pour and spaced horizontally and vertically six inches on center; rods will be tied or welded at the intersections. The reinforcing is to be anchored into the ceiling and floor to a minimum depth of one-half the thickness of the adjoining member.

b. Modular vaults meeting UL standards may be used in lieu of 1.a above.

c. ***Steel-lined Construction.*** Where unique structural circumstances do not permit concrete construction of a vault, construction will be of steel alloy-type, such as US Steel T-1, having characteristics of high yield and tensile strength. (If alloy-type steel is not available, normal structural steel may be used, but in a minimum thickness of 1/4 inch). The metal plates are to be continuously welded to load-bearing steel members of a thickness equal to that of the plates. If the load-bearing steel members are being placed in a continuous floor and ceiling of reinforced concrete, they must be firmly affixed to a depth of one-half the thickness of the floor and ceiling. If the floor and/or ceiling construction is less than six inches of reinforced concrete, a steel liner is to be constructed the same as the walls to form the floor and ceiling of the vault. Seams where the steel plates meet horizontally and vertically are to be continuously welded together.

d. ***All vaults will be equipped with a GSA-approved Class 5 vault door.*** Normally, within the United States a vault will have only one door that serves as both entrance and exit from the SCIF. If the travel distance from the most remote point in the SCIF to the door exceeds 50 feet, a second door equal to the original door, must be installed for life safety purposes. Travel distance will be measured on the floor along the natural path of travel, starting one foot from the most remote point, curving around any corners or obstructions, and ending at the entrance doorway. When a SCIF has more than one door, only one should be used for normal business.

2. SCIF Criteria For Permanent Construction

Walls, floor, and ceiling will be permanently contructed and attached to each other. To provide visual evidence of attempted entry, all construction must be done in a workmanlike manner, properly finished, and/or painted. This facility is acceptable for the following:

a. Inside the United States, ground level:

(1) Closed storage on a military installation or equivalent.

(2) Open storage on a military installation or equivalent if facility is alarmed and located in a building that has continuous personnel access control, 24-hour guard force, and reserve guard force.

APPROVED FOR RELEASE
DATE: NOV 2000

(3) Continuous operations.

(4) Secure working area.

b. Inside the United States, above or below ground level:

(1) Closed storage.

(2) Open storage if facility is alarmed and located in a building that has continuous personnel access control, 24-hour guard force, and reserve guard force.

(3) Continuous operations.

(4) Secure working area.

c. Outside the United States:

Continuous operations on a military reservation or equivalent, with prior approval of the SOIC.

3. SCIF Construction Criteria For Steel Plate

Walls, ceilings, and floors to be reinforced on the inside with steel plate not less than 1/8 inch thick. The plates at all vertical joints are to be affixed to vertical steel members of a thickness not less than that of the plates. The vertical plates will be spot welded to the vertical members by applying a 1 inch long weld every 12 inches; meeting of the plates in the horizontal plane will be continuously welded. Floor and ceiling reinforcements must be securely affixed to the walls with steel angles welded or bolted in place. Walls, ceiling, and floors of reinforced concrete at least 4 inches thick or of solid masonry (stone or brick) at least 8 inches thick are adequate. Existing walls, ceilings, and floors of hollow masonry (blocks and tiles) or lesser materials not meeting this criteria must be reinforced with steel plating 1/8 inch thick. This facility is acceptable for the following overseas applications:

a. Outside the United States:

(1) Closed storage.

(2) Continuous operations.

b. Inside the United States:

Not applicable.

4. SCIF Construction Criteria For Expanded Metal

Walls to be reinforced, slab to slab, with 9-gauge expanded metal. The expanded metal will be spot welded every 6 inches to vertical and horizontal metal supports of equal or greater thickness that have been solidly and permanently attached to the true floor and true ceiling. Floors and ceilings that are of masonry or metal construction require no special treatment. This facility is acceptable for the following applications:

a. Inside the United States, ground level:

(1) Closed storage.

(2) Open storage if facility is alarmed and located in a building that has continuous personnel access control, 24-hour guard force, and reserve guard force.

b. Outside the Unites States:

Closed storage on a military reservation or equivalent, with prior approval of the SOIC.

APPROVED FOR RELEASE
DATE: NOV 2000

B. MINIMUMS

The above provides minimum specifications. The use of materials having thickness or diameters larger than those specified is permissible. The terms "anchored to and/or embedded into the floor and ceiling" may apply to the affixing of supporting members and reinforcing to the true slab or to the most solid surfaces; however, subfloors and false ceilings are not to be used for this purpose.

C. WINDOWS

1. All windows that might reasonably afford visual surveillance of activity within will be made opaque or equipped with blinds, drapes, or other coverings to preclude such visual surveillance.

2. Inside the United States

Windows at ground level or readily accessible from the ground normally will be equipped with metal grills or bars. SCIFs located within fenced and guarded military compounds or equivalent may eliminate this requirement if the windows are made nonopenable by either permanently sealing them or equipping them on the inside with deadbolt locking mechanisms. For SCIFs having open storage and/or located in a high crime or risk area, or in one that is subject to civil disorders, metal grills or bars will be used. Windows above ground level and not accessible need only be lockable from the inside with deadbolt lock mechanisms. In open storage conditions at ground level, consideration should be given to sealing the windows by filling with brick/mortar or affixing lockable steel shutters to the windows.

3. Outside of the United States

All windows will be protected against forced entry with steel bars, except when located within fenced and guarded military compounds or equivalent where the CSA may waive this requirement.

D. MINIMUM SPECIFICATION FOR ENTRANCE, EXIT, AND ACCESS DOORS

1. All doors must be plumbed in their frames and the frame firmly affixed to the surrounding wall.

2. All SCIF entrance doors must be equipped with a door closer, Group I combination lock, and an access control device. Doors with hinges exposed must be modified with nonremovable pins or by installation of "dog bolts" or security studs. (NOTE: The specification does not apply to the GSA-approved Class 5 and 6 vault doors. These doors are secure as designed, must be used as specified in this document, and are not suitable for the installation of door closers, access control devices, or panic hardware.)

3. SCIF exit doors, when required, must be the same or equal to the entrance door. The door will be secured with "deadbolt" panic hardware on the inside and have no exterior hardware. Where life-safety codes permit, a sliding "deadbolt" should be installed, in addition to the panic hardware, and secured when the SCIF is unoccupied.

4. For entrance and exit doors, when life-safety codes dictate that panic hardware must exist on the door and the normally accepted extension #50 escape device is disallowed, an additional like door without frontal hardware will be installed to facilitate the use of panic hardware.

5. Details of specific manufacturers and models of approved combination locks, access control devices, and other related hardware is covered in the technical annex furnished by CSA.

APPROVED FOR RELEASE
DATE: NOV 2000

6. **SCIFs inside the United States** may be equipped with either a Class 5 or 6 vault door; a metal-clad fire door, minimum of 16-gauge metal; a solid core wood door, minimum of 1 3/4 inches; or flat-sill fire door with built-in boltwork.

7. **SCIFs outside the United States** must be equipped with a GSA-approved Class 5 or 6 vault door, or a locally fabricated door and frame equal to the steel reinforcement required in Section V.A.3 or V.A.4 depending on the type of SCIF. (NOTE: Specifications for locally fabricated doors are covered in the technical annex furnished by CSA.)

E. PHYSICAL PROTECTION OF VENTS AND DUCTS

1. All vents, ducts, and similar openings in excess of 90 square inches that enter or pass through a SCIF must be blocked with either bars, grills, or commercial metal duct sound baffles that meet one of the sound attenuation classes. If bars are used, they must be 1/2 inch diameter steel, welded vertically and horizontally, 6 inches on center; if grills are used, they must be of 9-gauge expanded steel; if commercial sound baffles are used, the baffles or wave forms must be metal, permanently installed and no farther apart than 6 inches in one dimension.

2. All vents and ducts must have a nonconductive section (a piece of dissimilar material unable to carry electric current) installed at the perimeter of the SCIF. An access port to allow inspection of the protection in the vent or duct must be installed inside the secure perimeter of the SCIF. The access port itself must be able to be secured by padlock or other approved device.

3. **SCIFs located inside the United States**
An alarm may be installed in lieu of bars or grills, depending on requirements of the CSA. Sound baffles may also be required by the CSA.

4. **SCIFs located outside of the United States**
Bars of 1/2 inch diameter steel, welded vertically and horizontally, 6 inches on center, must be used in addition to other requirements of the CSA.

APPROVED FOR RELEASE
DATE: NOV 2000

SECTION VI

TEMPORARY SECURE WORKING AREA (TSWA)

A temporary secure working area is defined as a temporarily accredited facility that is used no more than 40 hours monthly for the handling, discussing, and/or processing of SCI, but where SCI will not be stored.

During the entire period the TSWA is in use, the entrance will be controlled and access limited to persons having the clearance for which the area has been approved. Approval for using such areas must be obtained from the SOIC of the next higher level within appropriate SCI channels, setting forth room number(s), building, location, purpose, and specific security measures employed during usage as well as during other periods. TSWAs should be covered by an alarm system where possible. These areas will not be used for periods exceeding an average total of 40 hours per month. No special construction is required other than to meet sound attenuation requirements. If such a facility must also be used for the discussion of SCI, a technical surveillance countermeasures survey will be conducted periodically on a random basis during the operation of the temporary facility.

APPROVED FOR RELEASE
DATE: NOV 2000

SECTION VII

TELEPHONE SECURITY

One of the most serious technical security liabilities of the modern office environment is the presence of telephones connected to uncontrolled lines. The vulnerabilities inherent in telephone equipment are repeatedly encountered. The protection of telephone systems from on-hook audio exploitation constitutes a major element of the government's technical security program. Appropriate care in the selection and installation of telephone systems, and effective technical surveillance countermeasures examination procedures, must be treated as being of paramount importance for sensitive discussion areas.

Specific detailed instructions explaining the telephone audio security measures that are mandatory for SCIFs, and the options available for implementing them, are provided in the TELEPHONE SECURITY ANNEX to this manual.

The on-hook telephone audio security requirements for SCIFs are based on applications of technical standards developed and published by the Telephone Security Group (TSG), Countermeasures Subcommittee, Technical Surveillance Countermeasures Committee. TSG is the primary technical and policy resource in the US Intelligence Community for all aspects of the Technical Surveillance Countermeasures (TSCM) program that involve telephones and/or telephone systems.

TSG technical standards are developed and updated to extend the benefits obtained from ongoing studies and research programs. It is essential that all users of the TELEPHONE SECURITY ANNEX employ only the latest issues of applicable TSG standards. Only facilities that conform to the standards current at the time of installation will qualify for accreditation and grandfathering. To ensure that the latest versions of the TSG standards are used, direct all inquiries to the CSA.

APPROVED FOR RELEASE
DATE: NOV 2000

ANNEX A

MANUAL FOR PHYSICAL SECURITY STANDARDS FOR SENSITIVE COMPARTMENTED INFORMATION FACILITIES (SCIFs)

Supplement to DCID 1/21

(Effective 5 October 1989)

1. PURPOSE

This Annex specifies the requirements and procedures for systematically incorporating Telephone Security Group (TSG) approved telephone security measures into the planning, installation, maintenance, and management of telephone service for SCIFs.

2. APPLICABILITY AND SCOPE

a. The protective security measures contained herein address only the on-hook and unattended off-hook telephone security requirements for sensitive discussion areas.

b. Compliance with these security measures is mandatory for SCIF accreditation. This Annex neither prohibits implementation of more stringent local directives nor satisfies the requirements of other security programs such as Communications Security (COMSEC) or TEMPEST.

c. The telephone security measures of this Annex apply to the following types of equipment:

(1) Telephone instruments used with administrative telephone service.

(2) Voice terminals that connect to telecommunications links extending to areas for which continuous physical protection cannot be assured. Secure-voice telephones isolated from unprotected links by external encryption devices are not included.

(3) Internal communication (intercom) units unless an approved part of a system certified for secure use.

3. REFERENCES

a. TSG Standard 1, *Introduction to Telephone Security.*

b. TSG Standard 2, *TSG Guidelines for Computerized Telephone Systems.*

c. TSG Standard 3, *Type-Acceptance Program for Telephones Used With the Conventional Central Office Interface.*

d. TSG Standard 4, *Type-Acceptance Program for Electronic Telephones Used in Computerized Telephone Systems.*

e. TSG Standard 5, *On-Hook Telephone Audio Security Performance Specifications.*

f. TSG Standard 6, *Telephone Security Group Approved Equipment.*

TSG Standards are available to all members of the United States Intelligence Community from their respective Cognizant Security Authorities (CSAs). Individual standards may be released to nongovernment personnel who need them to accomplish work required by the US Government. Any such release is to be accompanied by a letter identifying the standard as an official government document that may not be disseminated further without specific approval of the issuing agency.

APPROVED FOR RELEASE
DATE: NOV 2000

4. RESPONSIBILITIES:

a. TSG. The TSG is responsible for evaluating on-hook audio security characteristics of telephone equipment and providing guidance on utilization and audio security countermeasures.

b. CSA. The CSA is responsible for ensuring compliance with TSG standards for all administrative telephone installations. The CSA will provide assistance to Special Security Officers (SSOs) in selection of authorized equipment. The CSA will maintain a current set of TSG standards.

c. SSO. The SSO is responsible for maintaining the integrity of installed administrative systems by:

(1) Ensuring that equipment is repaired expeditiously.

(2) Requesting technical surveillance countermeasures (TSCM) inspections for new systems and reinspections of significant expansions or modifications made to existing systems. To facilitate TSCM inspections, the SSO will maintain a log of all maintenance actions since the last TSCM inspection.

5. DEFINITIONS

a. Administrative Telephone. A telephone intended for unclassified conversation. This designation specifically excludes secure-voice systems unless they incorporate a non-secure mode of operation.

b. Disconnect Device. A device that has been accepted by the TSG as a means to disconnect, for security purposes, an on-hook station or computerized telephone system (CTS) from wires exiting the protected area. The disconnect device may be automatic or manual. A TSG-approved external ringer is normally required on the Central Office side of the disconnect device. (See TSG Standard 6.)

c. Isolator. A device or assembly of devices that has been accepted by the TSG as a means to isolate, for security purposes, an on-hook station or CTS from wires exiting the protected area. The isolation device must operate automatically and be transparent to the telephone and user. (See TSG Standard 6.)

d. On-Hook. In this condition, the telephone's handset is in the instrument's cradle and the associated circuit is deactivated; the telephone is hung-up. In the case of special purpose equipment, it is in its normal rest state and is not actively being used for communications.

e. Technical Surveillance Countermeasures (TSCM). Security measures taken to prevent and/or detect the installation of technical surveillance devices and/or the exploitation of security vulnerabilities.

f. Telecommunications Link. Any means used for the transmission of electrical or electromagnetic signals (e.g., wirelines, radiofrequency, fiber-optic).

g. TSG. The primary technical and policy resource in the National Advisory Group (NAG) structure for all aspects of the TSCM program that involves telephones and/or telephone systems.

h. Type-Accepted Telephones. Telephones that incorporate security measures that are intrinsic to the telephone itself. Their design and construction are known to comply with the on-hook security standards set by the TSG for telephone security classes 1, 2, or 3. (See TSG Standards 3 and 4).

i. Unattended, Off-hook Audio Security. Security measures intended to prevent the compromise of background conversations when the user temporarily leaves the instrument off-hook. (See TSG Standard 1.)

APPROVED FOR RELEASE
DATE: NOV 2000

6. REQUIREMENTS

a. Cable Control

All telephone wires must enter the SCIF through a common opening. Each conductor must be accurately accounted for from the point of entry. The accountability will identify, through labeling and/or log/journal entries, the precise use of every conductor. Excess conductors will be removed. Where removal is not feasible, they will be stripped, bound together, and grounded. This ground will not be associated with any classified information processing equipment or TEMPEST security equipment.

b. Access Control

Installation and maintenance personnel will possess the appropriate security clearance (determined by the CSA). If obtaining cleared personnel adversely affects the mission, technically qualified escorts will monitor the work performed. Access to telephone equipment and wiring within the SCIF must be controlled by SCIF personnel. Cleared or uncleared maintenance personnel given access to the SCIF should be US citizens.

c. On-Hook Audio Security

(1) Every telephone inside a SCIF must be provided approved and verifiable on-hook telephone audio security. There are two alternative methods authorized for providing this security: type-accepted telephones or line isolation. A registry (including ordering information) of currently available type-accepted telephones and TSG-approved security equipment is available from the CSA.

(a) Any telephone that has been type-accepted by TSG for telephone security classes 1, 2, or 3 may be installed in a SCIF without further on-hook audio security measures. TSG operates an open-ended telephone type-acceptance program. New telephones can be submitted for evaluation in accordance with TSG Standards 3 and 4, and accepted at any time.

(b) Line isolation may be accomplished by the use of an approved isolator or disconnect device (see TSG Standard 6), or it may be effected by a controlled CTS (see TSG Standard 2).

(2) Where both type-accepted telephones and isolation/disconnect measures are possible, it is not necessary to use both. Neither approach is regarded as being better than the other. The SCIF's specific needs will dictate the methods employed. (See TSG Standard 1.)

d. Off-Hook Audio Security

Unattended, off-hook security will be accomplished by one of the following:

(1) A hold feature that does not allow audio from the telephone to leave the SCIF perimeter. This can be accomplished by:

(a) A hold feature provided by a controlled CTS. (See TSG Standard 2.)

(b) A hold internal to the telephone that prevents audio from exiting the telephone when the hold feature is activated.

(c) A hold feature that allows the handset to be cradled when the hold feature is activated.

(2) A push-to-operate handset will be required if an appropriate hold feature is not available. (See TSG Standard 6.)

APPROVED FOR RELEASE
DATE: NOV 2000

e. Restricted Items

(1) Speakerphones are designed to pick up and transmit nearby conversation when they are in use. Therefore, speakerphones are expressly prohibited from common-use office areas where sensitive conversations might be intercepted.

(2) TSG-approved telephone answering devices may be installed in SCIFs only with prior approval of the CSA.

f. Prohibitions

(1) No equipment or device may be connected to an unprotected telephone line unless it has been specifically approved by TSG for such usage.

(2) Personally owned telecommunications equipment is not permitted in a SCIF.

(3) All additions of equipment or modifications to a SCIF's approved telecommunications system are prohibited except for the expansions or reconfigurations listed below:

(a) Additional telephones of the same type and under the same conditions already approved for use in the SCIF may be installed.

(b) Telephones may be removed from service.

(c) Telephones may be relocated within the SCIF as long as the new configuration does not degrade compliance with any of the terms of DCID 1/21.

g. Special Cases

Any alternative to these telephone security requirements may be submitted through the CSA for TSG evaluation. Proposed alternatives will be evaluated for approval based on their equivalency to the requirements cited within this Annex.

APPROVED FOR RELEASE
DATE: NOV 2000

[redacted]

ANNEX B

MANUAL FOR PHYSICAL SECURITY STANDARDS FOR SENSITIVE COMPARTMENTED INFORMATION FACILITIES (SCIFs)

Supplement to DCID 1/21

(Effective 15 August 1991)

This annex amplifies the requirements contained in Section IV, DCID 1/21 supplement, Manual for Physical Security Standards for Sensitive Compartmented Information Facilities, 1 September 1987, and establishes the minimum standards for intrusion detection systems for all SCIFs throughout government and for government-sponsored contractor facilities. Compliance with these standards is mandatory for all facilities established after the effective date of this annex, including any renovation of existing facilities insofar as the renovation will permit reasonable and practical upgrading, as determined by the cognizant security authority.

Any conflict with the security alarm requirements contained in Section IV, DCID 1/21 supplement, will be resolved in favor of this annex.

APPROVED FOR RELEASE
DATE: NOV 2000

ANNEX B

MANUAL FOR PHYSICAL SECURITY STANDARDS FOR SENSITIVE COMPARTMENTED INFORMATION FACILITIES (SCIFs)

Supplement to DCID 1/21

(Effective 15 August 1991)

1. CONCEPT

a. An Intrusion Detection System (IDS) detects an attempted or actual entry into the protected area. It must:

(1) Detect a forced entry.

(2) Detect a highly skilled surreptitious entry.

b. An IDS complements other physical security measures. It augments a guard force by extending its range of supervision over protected areas. An IDS consists of three essential components:

(1) Intrusion Detection Equipment (IDE).

(2) Security and response force personnel.

(3) Operating procedures.

2. OPERATION

a. IDS components operate in concert as a system with four distinct phases:

(1) Detection.

(2) Reporting.

(3) Assessment.

(4) Response.

b. These elements are equally important, and none can be eliminated if an IDS is to provide an acceptable degree of protection.

(1) Detection. The detection phase begins as soon as a detector or sensor reacts to stimuli it is designed to detect. The sensor alarm condition is then transmitted over cabling located within the protected area, called the detection loop, to the premise control unit (PCU). The PCU may service many sensors. The PCU and the sensors it serves comprise a "zone."

(2) Reporting. The PCU receives signals from all sensors in a protected area and incorporates these signals into a communications scheme. Another signal is added to the communication for supervision to prevent compromise of the communications scheme. This supervised signal is intended to disguise the information and protect the IDS against tampering or injection of false information by an intruder. The supervised signal is sent by the PCU via the transmission link to the monitor station. Inside the station either a dedicated panel or central processor monitors information from the PCU signals. When alarms occur, an annunciator generates an audible and visible alert to security personnel. Alarms result normally from intrusion, tampering, component failure, or system power failure.

APPROVED FOR RELEASE
DATE: NOV 2000

(3) Assessment. The assessment period is the first phase that requires human interaction. When alarm conditions occur, the operator assesses the situation and dispatches the response force.

(4) Response. The response phase begins as soon as the operator assesses an alarm condition. A response force must immediately respond to all alarms. Additionally, it must determine the precise nature of the alarm and take all measures necessary to safeguard the SCIF.

3. REQUIREMENTS

a. All areas of a SCIF shall be protected by an IDS unless continually occupied.

b. Acceptance of Equipment. All IDE must be UL-listed (or equivalent as defined by the cognizant security authority [CSA]) and approved by the CSA. Vendors may submit their IDE requests either through a Special Security Officer/Contractor Special Security Officer (SSO/CSSO) or directly to the CSA. Vendors must provide a UL certificate for installation and service (UL 611, 681, and 1076 apply) directly to the CSA for acceptance. Government installed, maintained, or furnished systems are subject to approval only by the CSA.

c. Responsibility for Proposals. All requests for acceptance must describe the IDE fully and include the results of testing by an independent laboratory. An independent laboratory evaluates the manufacturer's compliance to performance specifications. A request for acceptance of line supervision using data encryption standard (DES) must also include validation from the National Institute of Standards and Technology (NIST) or another independent testing laboratory recognized by the CSA. The description must identify the manufacturer and model of equipment and show how the IDE meets CSA and/or UL standards. Unless previously evaluated by the CSA, detailed circuit diagrams, theory of operation, system layout, distribution and communication schemes, and results of laboratory tests must be included in these requests to avoid delay in the evaluation process. The manufacturer must notify the CSA before modifying IDE that has received earlier CSA acceptance and document this modification. The CSA will return the results of the evaluation to the authorized requester. Results of IDE evaluations will remain on file with the CSA. Determination of CSA acceptance does not impart any obligation on the government to procure IDE.

d. Preinstallation Approval of IDS. The CSA will approve a proposed IDS before its installation within a SCIF as part of the initial SCIF construction approval process. A proposal for an IDS will be examined for the type and employment of accepted equipment. An IDS proposal will be submitted as part of a preconstruction approval process.

e. Equipment

(1) Transmission Line Security. Only Class I or Class II (referred to as "Class A" and "Class B" in Section IV of the DCID 1/21 supplement), CSA accepted line security shall be used. When the transmission line leaves the SCIF and traverses an uncontrolled area, it should be protected with Class I line supervision. With sufficient justification, the CSA may approve use of Class II line supervision. When the transmission line remains within the SCIF or a US SECRET-controlled area contiguous to the SCIF, Class II line supervision may be used.

(a) Class I. Class I line security is achieved through the use of DES or an algorithm based on the cypher feedback or cypher block chaining mode of encryption. Certification by NIST or another independent testing laboratory is required. The certificate must be retained by the CSA for the duration of operation of the SCIF.

APPROVED FOR RELEASE
DATE: NOV 2000

(b) Class II. Class II line supervision refers to systems in which the transmission is based on pseudorandom generated tones or digital encoding using an interrogation and response scheme throughout the entire communication, or UL Class AA line supervision. The signal shall not repeat itself within a minimum six-month period. Class II security shall be impervious to compromise using resistance, voltage, current, or signal substitution techniques.

(2) Internal Cabling. The cabling between the sensors and the PCU, termed the detection loop, must be dedicated to IDE and may be routed in rigid pipe (EMT or PVC) or equivalent raceways and must comply to national electric code standards. If applicable, the cabling must be installed in accordance with TEMPEST requirements. Internal cabling within the SCIF may be wire or fiber-optic cable. Radiofrequency/free space communications are prohibited within the SCIF.

(3) Restriction on Integration of Access Controls into SCIF IDSs. If an access control system is integrated into an IDS, reports from the access control system will be separate and subordinate in priority to reports from intrusion alarms.

(4) Maintenance Mode. When an alarm zone is placed in the maintenance mode, this condition will be signaled automatically to the monitor station. This signal must appear as an alarm or maintenance message at the monitor station. However, the alarm or message must continue visibly at the monitor station throughout the period of maintenance. A standard operating procedure (SOP) must be established to address appropriate actions when maintenance access is indicated at the panel. All maintenance periods will be archived in the system. The CSA may require that the maintenance personal identification number be established and controlled by the customer. The IDE will not contain any capability for remote diagnostics, maintenance, or programming, except for an alarm remote test feature at the monitor station. A self-test feature will be limited to one second per occurrence.

(5) Annunciation of Shunting or Masking Condition. Shunting or masking of any zone or sensor must be appropriately logged or recorded in archive. A shunted or masked zone or sensor must be displayed as such at the monitor station throughout the period the condition exists whenever there is a survey of zones or sensors.

(6) Alarms Indications. Indications of alarm status shall be revealed at the monitoring station and optionally within the confines of the SCIF. Where there is an operations security concern, the alarm monitoring panel shall be designed to prevent observation by unauthorized persons.

(7) Power Supplies. Primary power for all IDE will be commercial AC or DC power. In the event of commercial power failure at the protected area or monitor station, the equipment will change power sources without causing an alarm.

(a) Emergency Power. Emergency power must be capable of operating the IDE for a minimum of six hours. Emergency power may consist of a combination of battery and generator power. When batteries are used for emergency power, they will be maintained at full charge by automatic charging circuits. The emergency power system will comply with UL 603 and be tested for a six-hour period at least once a year by turning off or disconnecting the primary power system. Results of the tests will be maintained as required in paragraph 3.h., Procedures.

(b) Power Source and Failure Indication. An illuminated indication will exist at the PCU of the power source in use (AC or DC). Equipment at the monitor station will indicate visibly and audibly a failure in power source, a change in power source, and the location of the failure or change.

APPROVED FOR RELEASE
DATE: NOV 2000

(8) Tamper Protection. All IDE within the SCIF with removable covers will be equipped with tamper switches. The tamper detection will be monitored continuously whether the IDS is in the access or secure mode of operation.

(9) Prohibition Against Fortuitous Conduction via IDE. No IDE will be employed that allows audio and intelligence-bearing signals to pass out of the SCIF in any form.

(10) Safeguarding IDE

(a) In areas outside the US, IDE must remain solely under US control, or as otherwise authorized by the CSA.

(b) Key variables and operational passwords will be safeguarded, disseminated, and controlled as determined by the CSA.

(c) The line security encryption scheme must be capable of being readily changed on demand.

(d) All IDE will be identified and labeled with the manufacturer's name, model number, and, if available, serial number. This information will be recorded and maintained by the SSO/CSSO.

f. Installation

(1) Dedicated Equipment. All SCIFs will have dedicated intrusion detection equipment and zones independent from other protected sites. When many alarmed areas are protected by one monitor station, audible and visible annunciations for SCIF zones must be clearly distinguishable from other annunciations. All sensors protecting the SCIF will be installed within the SCIF.

(2) Multiple Zones. If a SCIF consists of more than six rooms, or more than 5,000 square feet, it will be protected by two or more alarm zones each providing separate annunciations at the monitor station. Each zone must be specifically defined by an approved perimeter, unless structurally prohibitive.

(3) Access/Secure Switch and PCU. No capability will exist to allow changing the access status of the IDS from a location outside the SCIF. All PCUs must be located inside the SCIF and should be located near the SCIF entrance. SCIF personnel must initiate all changes in access and secure status. Operation of the PCU will be restricted by use of a device or procedure that verifies authorized use. In the secure mode, any entry into the SCIF shall cause an alarm to be transmitted immediately to the monitor station.

(4) Motion Detection Protection. All areas within the SCIF between the floor and ceiling will be protected with motion detection sensors, e.g., ultrasonic, passive infrared, etc. Use of dual technology transmits an alarm condition independently from the other technology. A failed detector will cause an immediate and continuous alarm condition. Detection equipment must be installed in compliance with UL 681 and 1076, with the exception that the motion detector will alarm when two steps are taken within the detector's protective pattern.

(5) Accessible Areas. If a SCIF has a false ceiling or subfloor that provides a means for surreptitious entry, one of the following methods must be used to protect that area:

(a) A separate alarm zone, remaining in the secure mode at all times; or

(b) Reconstruction of those portions of the SCIF perimeter to acceptable physical and acoustic standards.

APPROVED FOR RELEASE
DATE: NOV 2000

(6) Protection of SCIF Perimeter Doors. Each SCIF perimeter door will be protected by a balanced magnetic switch (BMS) that meets the minimum standards of UL 634. The BMS must be installed in such a manner that an alarm signal will initiate before the nonhinged side of the door opens beyond 1/2 inch of the seated position. With the exception of the SCIF entrance, all SCIF door, window, and portal sensors shall remain activated and monitored and will receive response force service on a 24-hour basis. Emergency exit doors equipped with integrated life safety hardware may have the life safety alarm component integrated into the SCIF IDS as an additional detector. Emergency exit doors will be on a separate zone or assigned to zones that permit quick identification and response to the appropriate door when there is an alarm.

(7) Windows. All windows will be protected by an IDS, either independently or by the motion detection sensors in the room, as determined by the CSA.

(8) IDE Installation Criteria. All IDE will be installed in a manner to prevent access or removal from a location external to the SCIF and in compliance with UL 681 for "Installation of Burglar Alarm Equipment."

(9) IDS Requirements for Continuous Operations Facilities. A SCIF accredited for continuous operations may not require an IDS as determined by the CSA. A continuously operational SCIF must be staffed by sufficient personnel to ensure the integrity of the entire SCIF. This type of SCIF will be equipped with an alerting system if the occupants cannot observe all potential entrances into the SCIF. The system alerts occupants to an intrusion into the SCIF. An alert system will consist of BMSs or other appropriate sensors and will be connected to a signaling device through a closed loop to a latching relay. None of the IDE or cabling associated with the alert system will extend beyond the perimeter of the SCIF. A duress alarm(s) will be installed in the continuously occupied SCIF and be in the active mode at all times.

(10) False/Nuisance Alarm. Any alarm signal transmitted in the absence of a detected intrusion is a false alarm. A false alarm becomes a nuisance alarm when the effects of environment, equipment malfunction, operator failure, animals, electrical disturbances, and known effects cause the alarm to go off. All alarms shall be investigated and the results documented. The incidence of false/nuisance alarms should not exceed more than one in a period of 30 days throughout the entire IDS zone.

g. Personnel

(1) IDE Installation and Maintenance Personnel. Alarm installation and maintenance will be accomplished by individuals who possess a minimum of a DoD SECRET security clearance or who are US citizens with a favorable national agency check with inquiries (NACI). Use of foreign nationals or uncleared personnel for this purpose must have prior CSA approval.

(2) Monitor Station Staffing. The monitor station will be supervised continuously by individuals who possess a minimum of a DoD SECRET security clearance or who are US citizens with a favorable NACI. Use of foreign nationals or uncleared personnel for this purpose must have prior CSA approval. The duties of the operator will be documented and will entail observing monitor panels for reports of alarms and changes in IDE status, making accurate assessments of these reports, and dispatching the response force or notifying the appropriate authority in the event of an intrusion alarm. The operator will have no duties that interfere with the primary functions of monitoring alarms and dispatching the response force. A documented

APPROVED FOR RELEASE
DATE: NOV 2000

chain of authority will exist for use by security personnel during unusual situations. The operator will be trained sufficiently in the operation and theory of the IDE to properly interpret all incidents generated by the IDE. This training must also include all actions to be taken on receipt of an alarm activation.

h. Procedures

(1) Testing. SCIF IDS sensors will be tested semiannually at a minimum unless required more frequently by the CSA. All levels of emergency power will be tested in accordance with paragraph 3.e.(7) (a), Emergency Power. A record of IDE testing will be maintained at the SCIF that reflects: testing date, individuals who performed the test, specific equipment tested, malfunctions, and corrective actions taken. Tests of the response force will be conducted semiannually. The decision to test and manner of testing should be based on safety concerns and avoidance of degrading the effectiveness of the force's response to other duties. A record of response force testing will be maintained that describes: the identity of persons conducting the test, the effectiveness of the response, and any recommended changes to response procedures.

(2) Safeguarding IDS Plans. At a minimum, details of installed IDS will be controlled and restricted on a need-to-know basis.

(3) Operating Procedures. When the monitor station and response force are not controlled by the accredited SCIF, a written support agreement must be established.

(4) Alarm Condition Response. Every alarm condition will be treated initially as a detected intrusion until resolved by the response force. Response time to an alarm will not exceed:

Open Storage Area—five minutes.

Closed Storage Area—10 minutes.

The response force will investigate the source of an alarm and will notify SCIF personnel. The response force will take appropriate steps to safeguard the SCIF and prevent the escape of an intruder from the SCIF as permitted by SOP, local law enforcement, and circumstances until properly relieved.

(5) Catastrophic Failure. If the IDE suffers catastrophic failure, or loses primary and emergency power, SCIF-indoctrinated individuals must provide security by physically occupying the SCIF until the IDS can be made functional. As an alternative, the outside SCIF perimeter may be continuously protected by appropriately cleared guards, as determined by the CSA.

(6) IDS Logging. The IDS will incorporate a means for providing a historical record of all events, either automatically or through the use of a manual log system. If the IDE has no provision of automatic entry into archive, the operator will record the time, source, and type of alarm, and action taken. Results of investigations by the response force will be maintained at the monitor station. The historical records must be routinely reviewed by the responsible security officer. Records will be maintained for two years beyond the current year.

APPROVED FOR RELEASE
DATE: NOV 2000

ANNEX C

MANUAL FOR PHYSICAL SECURITY STANDARDS FOR SENSITIVE COMPARTMENTED INFORMATION FACILITIES

Supplement to DCID 1/21

(Effective 3 October 1990)

This annex pertains to specialized sensitive compartmented information facilities operating in a tactical environment. It is divided into three parts to reflect the accepted modes of tactical operation:

Part I - Ground Operation

Part II - Airborne Operation

Part III - Seaborne Operation

APPROVED FOR RELEASE
DATE: NOV 2000

Part I: Ground Operation

1. PURPOSE

This Annex prescribes the procedures for the physical security requirements for the operation of a sensitive compartmented information facility (SCIF) while in a field or tactical configuration, including training exercises.

2. APPLICABILITY AND SCOPE

Recognizing that field/tactical operations, as opposed to operations within a fixed military installation, are of the type considered least secure, the following minimum physical security requirements will be met and maintained. Situation and time permitting, these standards will be improved upon using the security considerations and requirements for permanent secure facilities as an ultimate goal. If available, permanent-type facilities will be used. Under field or combat conditions, a continuous 24-hour operation is mandatory. Every effort must be made to obtain the necessary support from the host command (e.g., security containers, vehicles, generators, fencing, weapons, etc.).

a. The SCIF will be located within the supported headquarters defensive perimeter, preferably adjacent to the Tactical Operations Center.

b. The SCIF will be located within a controlled area with a clearly marked perimeter, using a physical barrier (e.g., concertina, razorband, etc.).

c. The perimeter will be guarded by walking or fixed guards to provide observation of the entire controlled area. Guards will be armed with weapons and ammunition. The types of weapons will be prescribed by the supported commander.

d. Access to the controlled area will be restricted to a single gate/entrance, which will be guarded on a continuous basis.

e. An access list will be maintained, and access will be restricted to those personnel whose names appear on the list.

f. The SCIF will be occupied by a minimum of two SCI-cleared and -indoctrinated personnel at all times.

g. Emergency destruction and evacuation plans will be kept current.

h. SCI material will be stored in lockable containers when not in use.

i. Communications will be established and maintained with the backup guard force, if possible.

3. MOBILE SIGINT SCIF

a. The mobile SIGINT SCIF will be physically located at brigade or below.

b. A continuous 24-hour operation is mandatory.

c. The SCIF will be occupied by a minimum of two SCI-cleared and -indoctrinated personnel at all times.

APPROVED FOR RELEASE
DATE: NOV 2000

d. External physical security measures will be incorporated into the perimeter defense plans for the immediate area within which the facility is located.

(1) A physical barrier is not required as a prerequisite to establish a mobile SIGINT SCIF.

(2) External physical security controls will normally be a function of the personnel controlling the day-to-day operations of the facility.

e. Communications will be established and maintained with backup guard forces, if possible.

f. Emergency destruction plans will incorporate incendiary methods to ensure total destruction of SCI material in emergency situations.

g. A rigid side shelter or a portable van are two possible configurations that may be used.

(1) When a rigid side shelter or portable van is available, it is subject to the following additional restrictions:

(a) If it is a shelter, it will be mounted to a vehicle in such a way as to provide the facility with the capability of moving on short notice.

(b) A GSA-approved security container will be permanently affixed within the facility. The combination to the lock will be protected to the level of security of the material stored therein.

(c) Entrance to the facility will be controlled by SCI-indoctrinated personnel on duty within the facility. When situations occur when there are no SCI-indoctrinated personnel within the facility, i.e., during redeployment, classified material will be stored within the locked container and the exterior entrance to the facility will be secured.

(d) Entrance to the facility will be limited to SCI-indoctrinated personnel with an established need-to-know whenever SCI material is used within the facility.

(2) When a rigid side shelter or portable van is not available and a facility is required for operations, such as in the case of a soft side vehicle or man-portable system, it is subject to the following additional restrictions:

(a) Protection will consist of an opaque container, i.e., leather pouch, metal storage box, or other suitable container that prevents unauthorized viewing of the material.

(b) This container will be kept in the physical possession of an armed SCI-indoctrinated person.

(c) The container is subject to the two-person control rule.

h. The quantity of SCI material permitted within the facility will be limited to that which is absolutely essential to sustain the mission. Stringent security arrangements will be employed to ensure the quantity of SCI material is not allowed to accumulate more than is absolutely necessary.

(1) All working papers generated within the facility will be destroyed at the earliest possible time after they have served their mission support purpose to preclude accumulation of unnecessary classified material.

(2) If equipment is used to store or process SCI data, such equipment will meet the provisions of applicable directives for processing and destruction of classified material.

APPROVED FOR RELEASE
DATE: NOV 2000

Part II: Airborne Operation

1. PURPOSE

This Annex specifies the requirements for the security protection of aircraft utilizing sensitive compartmented information (SCI) while in the air or on the ground. These are minimum standards since each situation differs.

2. APPLICABILITY AND SCOPE

The criteria are applicable to all US Government- or contractor-owned mission aircraft transporting, using, or processing SCI material. This does not include commercial aircraft utilized to transport a designated courier.

3. DEFINITIONS

a. Temporary Secure Working Area. A temporarily accredited facility that is used no more than 40 hours monthly for handling, discussing, and/or processing SCI, but where SCI will not be stored.

b. Security Response Team (SRT). Individuals responsible for responding to an alarm or emergency.

c. Seal. A serially numbered device attached to an opening that if removed cannot be re-attached without showing evidence of its removal.

4. RESPONSIBILITIES

The cognizant security authority (CSA) is responsible for ensuring compliance with these standards and providing requisite SCI accreditation of SCIFs.

5. ACCREDITATION REQUIREMENTS

a. Parking and Patrol Requirements. Aircraft will generally be parked in an established restricted area with a security force, entry controls, and SRT support. In addition, periodic checks will be made of all hatches and seals (see security procedures below). Entry to the aircraft will be controlled by the air/ground crew or the aircraft commander, who must be properly cleared and indoctrinated for the level of SCI processed.

b. Restricted Area. When there is no established restricted area, a temporary restricted area must be established. A restricted area entry controller and a response team capable of a 5-minute response must be provided. Owner/user personnel will maintain surveillance over the aircraft during normal duty hours.

c. Security Procedures. When aircraft are parked, all hatches will be sealed to prevent unauthorized access from the exterior of the aircraft. Hatches that cannot be secured from the inside will be sealed using serially numbered seals. The seal numbers used will be furnished to the security force. The security force members will make periodic checks of seal numbers to ensure their integrity. Additionally, alarms will be installed where possible. All violations will be reported as security violations.

d. Alarm Systems. When SCI aircraft are protected by an approved alarm system, the entry controller stated above need not be posed. An SRT must be provided as stated above to respond to all alarms.

APPROVED FOR RELEASE
DATE: NOV 2000

e. Entry Authority Lists. The responsible official, as designated by the CSA, provides security force personnel with an entry authority list and seal numbers before departing from the immediate area of the aircraft. A security force supervisor authenticates the list and makes sure it is posted.

f. Protection of SCI Material. If possible, SCI material must be removed from the aircraft on mission completion or at unscheduled landings. When removal is not possible, or when suitable storage locations are not available, a minimum of two SCI-indoctrinated personnel must remain with the aircraft to control entry to the SCI compartment.

g. Destruction Requirements.

(1) An emergency action plan (EAP) that provides for the evacuation and/or destruction of classified material and equipment must be approved by the CSA and tested by a responsible official as designated by the CSA.

(2) Destruction devices such as hammers for equipment destruction and an approved shredder for destruction of other material must be on board in case the EAP must be initiated.

h. Non-US Airfields. On arrival, the responsible official as designated by the CSA is responsible for controlling the entry and maintaining surveillance over the aircraft until departure.

i. Nonmilitary Airfields. The local Federal Aviation Administration Security Officer will be notified of the estimated arrival time and security protection required. On arrival, the official, as designated by the CSA, is responsible for controlling entry and maintaining surveillance over the aircraft until departure.

j. Unfriendly Territory. If aircraft are forced to land in unfriendly territory, prepare SCI, crypto, and collateral classified material and equipment for immediate destruction. If possible, the destruction process should take place before landing. The decision to destroy is made by the Air Mission Supervisor. Cryptographic keying materials for SCI will be destroyed first, followed by all other SCI. When flights are planned over unfriendly territory during the conduct of official operations, SCI material carried on board will be carefully selected by the intelligence mission operational personnel on board to consist of the absolute minimum required for mission accomplishment. All personnel will rehearse emergency destruction before each mission.

APPROVED FOR RELEASE
DATE: NOV 2000

Part III: Seaborne Operation

1. PURPOSE

This Annex specifies the requirements for the construction and security protection of shipboard sensitive compartmented information facilities (S/SCIFs). It is not intended that existing, previously approved facilities be modified to conform with these standards.

2. APPLICABILITY AND SCOPE

a. The criteria are applicable to all new construction surface ships of the United States Navy, Air Force, Army, Marine Corps, and Coast Guard. The application of these criteria to submarines will be as specified by the Commander, Naval Intelligence Command (COMNAVINTCOM).

b. There may be instances in which circumstances constitute a threat of such proportion that they can only be offset by stringent security arrangements over and above those prescribed herein. Conversely, there may be instances in which time, location, mission, condition of use of the material, or other unforeseen factors may make full compliance with these standards unreasonable or impossible. These situations are to be referred to the cognizant security authority (CSA).

3. REFERENCES

Military Standard 1680B (Installation Criteria for Shipboard Secure Electrical Information Processing Systems) in conjunction with this Annex constitute the minimum physical security criteria applicable to S/SCIFs. MIL-STD-1680B is published by the Naval Sea Systems Command (NAVSEA).

4. DEFINITIONS

a. Permanent S/SCIF. An area used for handling, processing, and/or storage of SCI within a clearly defined physical perimeter barrier requiring "full-time" physical security protection. The area may contain one or more contiguous spaces requiring SCI accreditation. This type of facility is routinely utilized during both deployments and while in port.

b. Temporary S/SCIF. An area used for handling, processing, and/or storage of SCI within a clearly defined physical perimeter barrier requiring "temporary" physical security protection during deployments only. The area may contain one or more contiguous spaces requiring SCI accreditation. This type of facility is manned continuously by at least two appropriately indoctrinated personnel whenever there is cryptographic or SCI material present within the space. Prior to or at the completion of the mission, normally not to exceed one year, the facility will be deactivated and reported for disestablishment.

c. Temporary Secure Working Area. An area used for handling, processing, and/or limited storage of SCI within a clearly defined physical perimeter barrier on a "contingency" or "part-time" basis not to exceed a maximum average total of 40 hours per month. This type of facility is manned continuously by at least two appropriately indoctrinated personnel whenever there is cryptographic or SCI material within the space. Prior to or at the completion of the mission, normally not to exceed one year, the facility will be deactivated and reported for disestablishment.

APPROVED FOR RELEASE
DATE: NOV 2000

5. RESPONSIBILITIES

The CSA is responsible for ensuring compliance with these standards and providing requisite SCI accreditation of S/SCIFs.

6. PERMANENT S/SCIF ACCREDITATION

Ships requiring permanent accreditation will be processed for interim accreditation on completion of a physical security inspection and submission of a shipboard inspection checklist, which certifies its compliance with the following criteria. Final accreditation will be processed on favorable review of all SCI physical, administrative, ADP, and TEMPEST security requirements, if applicable.

a. Physical Perimeter Barrier. The physical perimeter barrier will be constructed or fabricated, or both, of aluminum or steel plate with a thickness not less than 0.125 inch. Nonoperable elements of the physical perimeter barrier will be fully braced and welded in place. (Note: Where several SCI spaces are contiguous to each other or non-SCI spaces in one complex, the entire complex may be enclosed by a single physical perimeter barrier conforming to this paragraph. Access to the complex will be from a single normal access door conforming to paragraph 6.b.; each compartment within the complex may have a separate access door from within the common physical perimeter barrier that need not be in compliance with paragraph 6.b. Access from such an SCI space to a contiguous SCI space may be via a door not in conformance with paragraph 5.b; however, access from such an SCI space to a contiguous non-SCI space will not be installed.)

b. Normal Access Door. The normal access door will be a shipboard vault-type door (in accordance with NAVSEA drawing 804-5184141) or a metal joiner door with honeycomb core (in accordance with NAVSEA drawing 805-46292) and will be fitted as specified below. Where the normal access door is in a bulkhead that is part of an air-tight perimeter, the airtight integrity may be maintained by colocating the airtight door with the vault door or by adding a vestibule.

(1) The manipulation, radiographic, and thermal resistant three-position tumbler combination lock will be equipped with a top reading dial, internal manual escape mechanism, and dial dust cover and be reinforced with a drill-resistant steel plate.

(2) In addition to the normal locking device, it will be equipped with a push-button, cipher-type electric or manual combination lock to be used as a latch and for access control only while the space is manned.

(3) The door will be equipped with a full-length astragal on the latching side to effectively protect the latch bolt from an unauthorized entry attempt.

(4) The door will be constructed in a manner that will preclude unauthorized removal of, and preferably hamper access to, hinge pins and anchor bolts as well as obstruct access to locking bolts between the door and frame.

c. Emergency Exit. The emergency exit door will be fabricated of steel or aluminum plate in consonance with the physical perimeter barrier as specified in paragraph 6.a. and mounted in a frame braced and welded in place in a manner commensurate with the structural characteristics of the bulkhead, deck, or overhead in which it is situated.

d. Restriction on Damage Control Fittings and Cables. Because of the security restrictions imposed in gaining access to these spaces, no essential damage control fittings or cables will be located within or pass through an SCI space.

APPROVED FOR RELEASE
DATE: NOV 2000

e. Removable Hatches and Deck Plates. Hatches and deck plates less than 10 square feet that are secured by exposed nuts and bolts (external to the SCI space) will be secured with externally attached, high-security padlocks (unless their weight or size makes removal unreasonable). The padlock keys will be stowed in a security container located within a space under appropriate security control.

f. Vent and Duct Barriers. Vents, ducts, or other physical perimeter barrier openings with a cross-sectional dimension greater than 96 square inches will be protected at the perimeter with a fixed man-proof barrier or security grille. The grille will be fabricated of steel or aluminum grating or bars with a thickness in consonance with the physical perimeter barrier (see paragraph 6.a.). If a grating is used, bridge center-to-center measurements will not exceed 1.42 inches by 4 inches. Barriers will be mounted on 6-inch centers. The grating or bars will be welded in place. This requirement is not applicable to through ducts that have no opening into the space.

g. Acoustical Isolation. The physical perimeter barrier of all SCI spaces will be sealed or insulated with nonhardening caulking material to prevent inadvertent disclosure of SCI discussions or briefings from within the space, taking into account the normal ambient noise level to persons located in adjacent passageways and/or compartments. In cases where the perimeter material installation does not sufficiently attenuate voices or sounds of activities originating SCI information, the ambient noise level will be raised by the use of sound masking or audio countermeasures devices, controllable sound-generating sources, or additional perimeter material installation. Air handling units and ducts will be equipped with silencers or sound countermeasures devices unless continuous duty blowers provide a practical, effective level of security masking (blower noise) in each air path. An effective level of security may be determined by placing appropriate personnel inside and outside the space to determine if SCI information can be overheard outside the space.

h. Visual Isolation. Doors, scuttles, vents, louvers, or other openings in the physical perimeter barrier through which the interior may be viewed will be screened or curtained.

i. Intrusion Detection System (IDS). The normal access door and emergency exit door(s) will be protected by a visual and audible alarm system. This system will comply with MIL-STD-1680B and provide a means of warning the space supervisor when a normal access door or emergency exit is opened. The installation will consist of visual and aural indicators located at the supervisor's position and connected to sensors at each door. The normal access door alarm may have a disconnect feature. Emergency exits will be connected to the alarm system at all times and will not have a disconnect feature installed. The IDS will be connected to a remote alarm monitor station that is colocated with other remote IDSs or in a space that is continuously manned by personnel capable of responding to an alarm at the protected space. Additionally, primary power of the IDS will be connected to an emergency lighting panel within the space. (Note: This requirement may not apply to SCI spaces under continuous manning by at least two appropriately indoctrinated personnel who have the capability of detecting forced or surreptitious entry.)

j. Passing Scuttles and Windows. Passing scuttles and windows/ports will not be installed between SCI spaces and any other space on the ship.

k. Location of Cryptographic Equipment. Online and offline cryptographic equipment and terminal equipment processing SCI information will be located within the SCI space.

APPROVED FOR RELEASE
DATE: NOV 2000

l. Secure Storage Containers. SCI material will be stored only in GSA-approved security containers or equal. Containers will be welded in place or otherwise secured to a foundation for safety and to prevent rapid removal.

m. Rotary or Tone Dial Telephones. Rotary or tone dial telephones, except the TA-866/STC-1, will be equipped with a push-to-operate feature and a manual line disconnect device such as the WECO plug 505A-61 and jack 549A-49 or equal. Shipboard telephone systems meeting the above criteria may be connected to shore telephone lines under the following conditions:

(1) All shipboard telephones access the portside central office (CO) lines via an intermediate switch (switchboard, computer-driven private branch exchange, or mechanical switches).

(2) Telephone lines between the intermediate switch and the dockside connecting device will be under the control of and maintained by the ship's company. SCI space line will be terminated (brought to common ground) within the space housing the intermediate switch.

(3) The intermediate switch may serve shipboard spaces other than the SCI space, provided the wire run between the switch and the SCI space is in electronic metallic tubing (EMT) (or via controlled space).

(4) All computer-driven switches will be of US design and manufacture.

(5) The compartment housing the intermediate switch will be established as a "Limited Access Area." When not occupied, the space will be secured with a tamper-proof hasp and combination padlock conforming to MIL-STD-1680B.

(Note: Rotary or tone dial telephone circuits installed within the electrical perimeter barrier of an accredited secure processing center will have their lines filtered in accordance with MIL-STD-1680B.)

n. Sound-Powered Telephones. Sound-powered telephones will be eliminated from SCI spaces insofar as possible. When required, those instruments that connect to locations outside of SCI space(s) will be in compliance with the following installation criteria:

(1) The telephone cable will not break out to jackboxes or switchboards or to telephone sets other than at the designated stations. The telephone cable will not be shared with any other circuit call or signal systems associated with this circuit.

(2) Sound-powered telephones will be equipped with a selector switch, located at the controlling station, capable of:

(a) disconnecting all stations,

(b) selecting any one station and disconnecting the remaining stations,

(c) a paralleled connection to all stations.

(3) Other stations that are accredited as SCI space not equipped with the selector switch in paragraph 6.n.(2) will have a positive disconnect device in the telephone line.

(4) Sound-powered telephone sets colocated in a space with this system, and not used for passing SCI information, will have a sign posted that these telephone sets are not for passing classified information.

(5) A call or signal system will be provided. Call signal station type IC/D, when used for circuit EM will be modified to provide a disconnect in the line to prevent a loudspeaker from functioning as a microphone.

APPROVED FOR RELEASE
DATE: NOV 2000

o. SCI Intercommunication Announcing System. An intercommunication-type announcing system processing SCI information, which connects to or passes through areas outside the SCI space, will be used in the 12MC system and be installed in accordance with MIL-STD-1680B. The switch matrix panel will be located within one of the SCI spaces. Primary AC power will be provided from a vital or emergency lighting circuit.

p. Supporting Intercommunication Announcing Systems. Intercommunication-type announcing systems installed within an SCI space, which do not process SCI information, will be designed or modified to provide the following physical or electrical security safeguards:

(1) Operational mode of the unit installed within the SCI space will limit operation to push-to-talk mode only.

(2) Receive elements will be equipped with a local amplifier as a "buffer" to prevent loudspeakers or earphones from functioning as microphones.

(3) Radio transmission capability for plain language radio telephones (excluding secure voice) will not be connected. Cable conductors assigned to the transmission of plain language radio telephones will be connected to a ground at each end of the cable.

(4) Equipment modified will have an appropriate field change label affixed to the unit that indicates the restriction. Additionally, the front panel will have a sign warning the user that the system is not for passing classified information.

q. Commercial Intercommunication Equipment. Commercial intercommunication equipment that does not have NAVSEA approval will not be installed in an SCI space.

r. General Announcing Systems. General announcing system loudspeakers will have an audio amplifier in the signal line to the loudspeaker to serve as a "buffer." The amplifier and the output signal lines will be installed within the SCI space.

s. Pneumatic Tube Systems. Pneumatic tube systems for passing SCI information will not be installed. Pneumatic tube systems previously installed will have the following characteristics:

(1) Locked cover at both ends.

(2) Capability to maintain the pressure or vacuum and lock it in the secure position at the initiating end.

(3) Direct voice intercommunication link between both ends (for example, telephone).

(4) Special color for the cartridges.

(5) Pneumatic tubes that run through passageways and are capable of being visually checked along their entire length.

t. Destruction Equipment. An effective and approved secure means of destruction of SCI material will be provided each SCI space or contiguous SCI spaces.

u. Emergency Power. An SCI space will have emergency power sufficient to operate destruction equipment, alarm systems, and access control devices and provide emergency lighting.

v. SCI Processing Systems. An SCI space that processes SCI electronically/electrically will be provided a visual TEMPEST inspection before activation.

7. TEMPORARY S/SCIF ACCREDITATION

Ships requiring temporary accreditation status will be processed for accreditation on completion of a physical security inspection and certification of compliance with the following

APPROVED FOR RELEASE
DATE: NOV 2000

physical security requirements. If the space is used to process SCI information electrically, it will be provided a visual TEMPEST inspection before activation and must comply with the full TEMPEST-related configuration control criteria of MIL-STD-1680B.

a. The physical perimeter barrier will consist of standard structural, structural nonsupport, or metal joiner bulkheads welded or riveted in place.

b. Doors will be at least metal joiner doors equipped with door closers and capable of being secured from the inside. Dutch doors are not acceptable. If cryptographic equipment is installed or stored within the space, and the space will be temporarily unmanned while cryptographic key material and/or SCI material are stored elsewhere, the door will be equipped with a tamper-proof hasp and combination padlock conforming to the requirements of MIL-STD-1680B.

c. Doors, scuttles, vents, louvers, or other openings in the perimeter that permit aural or visual penetration of the internal space will be screened, curtained, or blocked.

d. An effective and approved secure means of destruction of SCI material will be readily available in the space or nearby in general service spaces.

e. Cryptographic equipment processing SCI information will be located in the SCI space, or, if located in a secure processing center other than that accredited for SCI, will be electrically configured so as not to be compatible with the secure processing system of that secure processor.

f. A filing cabinet will be used for storage of SCI material.

g. Rotary or dial type telephones will be as specified in paragraph 6.m. above.

h. Sound-powered telephone installations will be as specified in paragraph 6.n. above.

8. TEMPORARY SECURE WORKING AREA (TSWA) ACCREDITATION

Ships requiring TSWA accreditation for "contingency" or "part-time" usage will be processed for accreditation on completion of a physical security inspection and certification of compliance with the following physical security requirements:

a. The physical perimeter barrier requires no special construction, provided it can prevent visual and aural access during all periods of SCI operation.

b. Doors will be capable of being secured from the inside.

c. Provisions will be made for posting a temporary sign that reads "RESTRICTED AREA—KEEP OUT—AUTHORIZED PERSONNEL ONLY."

d. When SCI material is to be stored in the space, a secure storage container conforming to MIL-STD-1680B will be provided. Security storage containers will be welded in place or otherwise secured to the foundation for safety and to prevent rapid removal.

e. The electrical security requirements for a TSWA space will be specified by NAVSEA on a selective basis.

9. EMBARKED PORTABLE SHIPBOARD COLLECTION VANS (PSCVs)

Ships requiring accreditation of embarked PSCVs may be activated on certification to GSA of compliance with the following physical security requirements. PSCVs are vans that are temporarily placed aboard the ship and are not part of the permanent structure.

a. The exterior surface of the van will be of solid construction and capable of showing evidence of physical penetration (except for intended passages for antenna cables, powerlines, etc.).

APPROVED FOR RELEASE
DATE: NOV 2000

b. The access door will fit securely and be equipped with a substantial locking device to secure the door from the inside in order to prevent forcible entry without tools.

c. Adequate measures will be established to preclude viewing of classified material by uncleared personnel.

d. Adequate provisions will be established to control the approach of uncleared personnel within the vicinity of the van. These measures will consist of instructions, promulgated by the station (ashore and afloat) in which the van is embarked, prohibiting loitering in the immediate vicinity of the van, and will include periodic visual security checks by appropriately indoctrinated personnel.

e. Adequate destruction equipment will be available and effective procedures established to ensure rapid and complete destruction of classified material in emergency situations.

f. All SCI material will be stored within the van and continuously manned by at least two appropriately indoctrinated personnel when activated for SCI support. If SCI material is to be stored outside the van, the space must be accredited by the CSA and be in compliance with this Annex.

g. The electrical security requirements for a PSCV will be specified by NAVSEA.

APPROVED FOR RELEASE
DATE: NOV 2000

i. Upon cessation of hostilities, all classified material will be returned to the parent element of the facility for reconciliation of records and destruction of obsolete material.

4. ESTABLISHING A TEMPORARY FIELD/TACTICAL SCIF

Frequently, tactical units will elect to set up nonpermanent SCIFs for processing SCI in support of ongoing field/tactical requirements. SCIFs established under these conditions will be secured in accordance with paragraphs 2.a. through 2.i. above. The Senior Intelligence Officer (SIO) of the military department (MILDEP) having SCI security responsibility over the activity is authorized to temporarily accredit such configurations, including point-to-point SCI communications circuits using low-power-level equipment, and may delegate that authority to the cognizant service special security office. Temporary facilities established in accordance with the provisions of this paragraph will not be authorized for operations to exceed 90 days. If the temporary SCIF contains communications equipment that has direct access to AUTOVON, or ADP equipment used for processing SCI material, TEMPEST security requirements also apply.

5. ESTABLISHING A TEMPORARY TACTICAL SCIF IN AN EXISTING PERMANENT BUILDING

a. Occupied Building. Accreditation of a temporary tactical SCIF in an existing permanent building occupied by other personnel shall be granted in accordance with paragraph 6, below.

b. Unoccupied Building. Accreditation of a temporary SCIF in an existing unoccupied permanent building will be granted in accordance with paragraph 4, above.

6. TEMPORARY RELOCATION OF PERMANENT FACILITIES

Permanently accredited SCIFs may be relocated to a field configuration as specified herein without a formal accreditation of the temporary SCIF. The SIO of the MILDEP or his designated representative, having SCI security responsibility over the activity, will be informed of all such relocations, to include the anticipated duration of the relocation and the physical security measures that will be in effect.

7. SEMIPERMANENT SCIFs

a. Vehicles used as tactical SCIFs may be used in nontactical situations if the SIO determines there is a need for more SCIF area and time and/or funds are not available to construct or enlarge a permanent SCIF. These types of SCIFs are SEMIPERMANENT SCIFs (SPSCIFs).

b. The SPSCIF will be accredited and operated in the same manner as a permanent SCIF. Requirements for TEMPEST and ADP accreditation apply.

c. The SPSCIF must be of rigid construction similar to a van, trailer, or transportable shelter. The building material must be of such composition to show visible evidence of forced entry. Vents and air ducts must be constructed to prevent surreptitious entry. The doors must be of solid construction and plumbed so the door forms a good acoustical seal. If installed, emergency exits/escape hatches must be constructed so they can only be opened from the interior of the SPSCIF.

d. The SPSCIF must be placed within a fenced compound on a military installation or equivalent, as determined by the cognizant security authority (CSA). The fence must meet or exceed the standards described for a hardened 8-foot chain link fence in Military Handbook 1031/1. The fence must be at least 10 feet from the SPSCIF and related buildings and equipment. The distance from the fence to the SPSCIF may have

APPROVED FOR RELEASE
DATE: NOV 2000

to be greater to provide acoustical security or to meet COMSEC or TEMPEST requirements. Access control to the fenced compound must be continuous. Red cabling between SCIFs and SPSCIFs must be installed in accordance with COMSEC and TEMPEST requirements.

e. All SPSCIFs must have one of the following locks on the main entrance door:

(1) Built-in three position combination Group 1R lock.

(2) Medeco D-10 High Security Dropbolt with body guard plate assembly or Medeco D-11 series deadbolt.

(3) S&G 8077A or B Combination padlock.

(4) Medeco Protector model D50-100-1/2 padlock.

(5) Medeco Protector model D50-200-1/2 padlock.

(6) CSA-approved equivalent lock to any of the above locks.

(NOTE: The keys to the padlocks and built-in key locks must be under two-person control at all times. This is due to expense of replacing locks with compromised keys.)

f. SPSCIFs do not need any additional security measures if one of the following exists:

(1) Continuous operations. Continuous operations exist when the SPSCIF is occupied by two SCI-indoctrinated persons 24 hours a day. When there are multiple vehicles/shelters within a fenced compound, only those occupied by two or more SCI-indoctrinated people qualify as continuous operation facilities.

(2) Dedicated guard force cleared to at least the SECRET level. The dedicated guard force must be present whenever the SPSCIF is not occupied and must have continuous surveillance of the SPSCIF entrances. The guard force must check the perimeter of the SPSCIF at least twice an hour at random intervals. Guard response time will be five minutes or less.

g. SPSCIFs not storing classified material and not meeting one of the requirements in the above paragraph must have an intrusion detection systems (IDS) as prescribed for permanent facilities.

h. Requirements for Storage:

(1) SCI material will not be stored in a SPSCIF except when removal is not feasible, i.e., computer hard disk.

(2) Storage in the United States and Outside the United States. If the facility does not have continuous operations or a dedicated guard force at the SPSCIF, a three-position Group 1R combination lock and an IDS for the SPSCIF interior and the SPSCIF compound is required. The interior SPSCIF IDS must be as prescribed for permanent SCIFs. The SPSCIF compound IDS must meet the same standards of the interior SPSCIF IDS, except the sensors may be ground sensors, motion detection CCTV, or other exterior perimeter or area sensors approved by the CSA.

8. REFERENCES

The policy and procedures for establishing SCIFs are outlined in DCID 1/21 or in this DCID 1/21 supplemental manual.

9. RESPONSIBILITIES

The Cognizant Security Authority is responsible for ensuring compliance with these standards and providing requisite SCI accreditation. The SIO is responsible when a temporary field or tactical SCIF is used in support of field training exercises.

APPROVED FOR RELEASE
DATE: NOV 2000